Network Device Interpretation # 202117

Time Data for vNDs

Status: ☒ *Active* ☐ *Inactive*

Date: *11-Jan-2022*

End of proposed Transition Period (to be updated after TR2TD process): *11-Feb-2022*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☒ *Network iTC*

Affected Document(s): *NDcPPv2.2e, ND SD2.2*

Affected Section(s): *FPT_STM_EXT.1.2*

Superseded Interpretation(s): *None*

Issue:

FPT_STM_EXT.1.2 allows for two selections with regards to how the TOE obtains time data:

- Allow the Security Administrator to set the time
- Synchronise time with an NTP server

If the second selection is made, the selection-based requirement FCS_NTP_EXT.1 must be claimed as the interface to an NTP server is considered to be inside the TOE boundary.

Application Note 35 states the following:

“For a vND, the virtualization system can be used as an external time source. It is assumed that the VS itself uses NTP or some other external source for its time, and that this time is made available to VMs.”

This application note is made for vNDs in general, and is not limited to a specific use case. Therefore, the CCTL believes that this application note is intended to apply to either Case 1 or Case 2 vNDs. This is specifically reinforced by the fact that the app note says “it is assumed…” which suggests the VS does not need to be part of the TOE boundary (otherwise an assumption would not be made since it is a testable assertion as part of the TSF). The CCTL also believes that this is covered by the A.VS_CORRECT_CONFIGURATION assumption, as being “correctly configured” can reasonably be assumed to apply to having a correctly configured clock that the TOE can rely on.

If the TOE is a Case 1 vND, where the TOE boundary only includes the vND and not the underlying VS, and the TOE is receiving its time data from the hypervisor, which is in turn assumed to get its time data from an environmental NTP server, what is the appropriate claim for FPT_STM_EXT.1.2? The

“synchronise time with an NTP server” selection does not make sense here because the NTP server interface on the hypervisor is outside the TOE boundary, so FCS_NTP_EXT.1 would not apply to the TOE. And the “allow the Security Administrator to set the time” selection could give the reader a misleading expectation that the TOE’s clock is completely arbitrary rather than being derived from an environmental source that ultimately does tie back to an NTP server.

This application note is made for vNDs in general, and is not limited to a specific use case. Therefore, the CCTL believes that this application note is intended to apply to either Case 1 or Case 2 vNDs. This is specifically reinforced by the fact that the app note says “it is assumed…” which suggests the VS does not need to be part of the TOE boundary (otherwise an assumption would not be made since it is a testable assertion as part of the TSF). The CCTL also believes that this is covered by the A.VS_CORRECT_CONFIGURATION assumption, as being “correctly configured” can reasonably be assumed to apply to having a correctly configured clock that the TOE can rely on.

If the TOE is a Case 1 vND, where the TOE boundary only includes the vND and not the underlying VS, and the TOE is receiving its time data from the hypervisor, which is in turn assumed to get its time data from an environmental NTP server, what is the appropriate claim for FPT_STM_EXT.1.2? The “synchronise time with an NTP server” selection does not make sense here because the NTP server interface on the hypervisor is outside the TOE boundary, so FCS_NTP_EXT.1 would not apply to the TOE. And the “allow the Security Administrator to set the time” selection could give the reader a misleading expectation that the TOE’s clock is completely arbitrary rather than being derived from an environmental source that ultimately does tie back to an NTP server.

Resolution:

The NIT acknowledges the inconsistency between the SFR, Application Note, and vND use case. The cPP and SD are updated as follows.

FTP_STM_EXT.1.2 shall be modified as follows:

<old>

FPT_STM_EXT.1.2 The TSF shall [selection: *allow the Security Administrator to set the time, synchronise time with an NTP server*].

</old>

<new>

FPT_STM_EXT.1.2 The TSF shall [selection: *allow the Security Administrator to set the time, synchronise time with an NTP server, obtain time from the underlying virtualization system*].

</new>

Application Note 35 paragraph 3 shall be modified as follows:

<old>

For a vND, the virtualization system can be used as an external time source. It is assumed that the VS itself uses NTP or some other external source for its time, and that this time is made available to VMs.

</old>

<new>

For a Case 1 vND, the virtualization system can be used as an external time source. For a Case 2 vND, the virtualization system is part of the TOE, so the time must be set by a security administrator or synchronized with an NTP server.

</new>

The following shall be appended to the TSS requirements for FPT_STM_EXT.1:

<new>

If "obtain time from the underlying virtualization system" is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.

</new>

The following shall be appended to the Guidance Documentation requirements for FPT_STM_EXT.1:

<new>

If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.

</new>

The following test shall be added for FPT_STM_EXT.1:

<new>

c) Test 3: [conditional] If the TOE obtains time from the underlying VS, the evaluator shall record the time on the TOE, modify the time on the underlying VS, and verify the modified time is reflected by the TOE. If there is a delay between the setting the time on the VS and when the time is reflected on the TOE, the evaluator shall ensure this delay is consistent with the TSS and Guidance.

</new>

Rationale:

The NIT does not add requirements to the cPP; however, the wording of the Application Note and the Case 1 vND use case clearly indicate obtaining time from the underlying virtualization system was an intended function.

Further Action:

None

Action by Network iTC:

None